MERLIN

Author Russel Van Tuyl
Twitter @merlin_c2
Email Russel.VanTuyl@gmail.com
GitHub github.com/Ne0nd0g/merlin
Medium Medium.com/@Ne0nd0g

Cross-platform post-exploitation HTTP/2 Command & Control server and agent written in Go

Merlin Server Executable Command Line Flags	
-debug	Enable debug output
-h	Print help menu
-i	The IP address of the interface to bind to
-p	Merlin Server Port
-proto	Protocol for the agent to connect with [h2, hq]
-v	Enable verbose output
-x509cert	The x509 certificate for the HTTPS listener
-x509key	The x509 certificate key for the HTTPS listener

Merlin Agent Executable Command Line Flags	
-debug	Enable debug output
-h	Print help menu
-proto	Protocol for the agent to connect with [h2, hq]
-sleep	Time for agent to sleep (default 30s)
-url	Full URL for agent to connect to
-v	Enable verbose output
-version	Print the agent version and exit

Merlin Server Agent Menu - Merlin[module][Invoke-Mimikatz]»	
back	Return to the main menu
info	Show information about a module
main	Return to the main menu
reload	Reloads the module to a fresh clean state
run	Run or execute the module
set	Set the value for one of the module's options
show	Show information about a module or its options Options: info, options

Merlin Server Main Menu - Merlin»	
agent	Interact with agents or list agents
banner	Print the Merlin banner
exit	Exit and close the Merlin Server
interact	Interact with an agent. Alias for Empire users
quit	Exit and close the Merlin Server
remove	Remove or delete a DEAD agent from the server
sessions	List all agents session information. Alias for MSF users
use	Use a function or module of Merlin
version	Print the Merlin server version
*	Anything else will be execute on the host operating sys-

Merlin Server Agent Menu - Merlin[agent][UUID]»	
cmd	Execute a command on the agent Example: cmd –c 3 ping 8.8.8.8
back	Return to the main menu
download	Download a file from the agent download <remote_file>
info	Display all information about the agent
kill	Instruct the agent to die or quit
main	Return to the main menu
set	Set the value for one of the agent’s options Options: maxretry, padding, skew, sleep
upload	Upload a file to the agent upload <local_file> <remote_file>

GitHub Directory Structure	
cmd	The main Merlin Server and Agent Go applications
data	Main directory used by and distributed with Merlin Server
data/agent/<uuid>/agent_logt.txt	Log file of all agent activity
data/bin/	Compiled Merlin Agent binaries for Windows (.exe & DLL), Linux, Mac, and Invoke-Merlin.ps1
data/html	Merlin JavaScript test HTML page and Merlin JavaScript Agent (merlin.js)
data/log/merlinServerLog.txt	Log file of all Merlin Server activity
data/modules	Module files in JSON format for agent actions. Dynamically add .json files during use
data/x509	Default location for server.crt and server.key files
docs	Holds templates for GitHub issues, pull requests, change log, & contributing guidelines
pkg	Source code files for Merlin
vendor	3rd party library files used with Merlin
LICENSE	GNU General Public License v3.0 Information
Makefile	GNU Make file for compiling Server or Agent

Highlights
Command tab completion for ease of use
Robust in application help menu
Verbose server and agent log files
Good Wiki: https://github.com/Ne0nd0g/merlin/wiki
C2 uses HTTP/2 and QUIC protocols for evasion
JavaScript, PowerShell, and DLL agents
Community Contributors: Dan Borges (@ahhh), Joel Braun (@twigatech) and Adam Cronan (@0xada4d)
Thanks to JetBrains for the GoLand IDE open source license

Agent Operational Configuration Settings	
maxretry	The amount of failed check in attempts before quitting
padding	Maximum size of C2 message padding size (in bytes) to evade message size based detection Example: set padding 8192
skew	Jitter time factor between check in attempts Example: set skew 5000
sleep	Amount of time between check in attempts Example: set sleep 63m

NOTES